

RM-304 AH-5 ES-17
August 1972

ON THE THEORY AND APPLICATION
OF SUM COMPOSITION OF LATIN SQUARES
AND ORTHOGONAL LATIN SQUARES (1)

A. Hedayat and E. Seiden
Florida State University
and
Michigan State University

- (1) Research was supported in part by 5R01-GM-05900 at Cornell University, Ithaca, New York.

1. Introduction.

This paper supersedes our previous papers [3], [4], [5], and [7]. Our object here is three-fold. First, to put the theory of "sum composition" of Latin squares and orthogonal Latin squares in its most precise form. Second, to compile and unify our previous results which have appeared in technical reports and also in a proceedings of a conference in Italy which are not readily available. And finally to present some new results in this area.

In short our research relates to the following question. Given two Latin squares L_1 and L_2 of order n_1 and n_2 ($n_1 \geq n_2$) respectively. In how many ways (if any at all) can one compose L_1 and L_2 in order to obtain a Latin square L_3 of order m , where m is a function of n_1 and n_2 only? It is well known that $L_3 = L_1 \otimes L_2$ is a Latin square of order $n_1 n_2$ irrespective of the combinatorial structures of L_1 and L_2 . Our theory produces a Latin square L_3 of order $n_1 + n_2$ provided L_1 has a certain combinatorial structure and thus the name "sum composition". Even though this method does not work for all pairs of Latin squares, it has an immediate application in the construction of orthogonal Latin squares with certain interesting and useful combinatorial structures including those of order $4t + 2$, $t \geq 2$. As will be seen this method is easy and simpler than other known methods for the construction of orthogonal Latin squares of order $4t + 2$ (see [1]). We also hope that the idea of sum composition can be extended to other combinatorial structures and designs.

We shall here highlight the content of this paper. In Section 2 we present the preliminary concepts and definitions which are then used in the following sections. Section 3 develops the basic idea of the sum composition of Latin squares. In this section we have also pointed out the usefulness of these concepts. Section 4 introduces the idea of horizontal and vertical projections of a given transversal on rows and columns. It also introduces the idea of capturing a lost transversal. It contains two lemmas for capturing a transversal by horizontal and vertical projections. These lemmas are

considered by us to be the "fundamental lemmas" in sum composition. In Section 5 we develop a technique which forms a basis for the construction of an $O(n,2)$ via sum composition of an $O(n_1,2)$ based on $GF(n_1)$ and an arbitrary $O(n_2,2)$. In Section 6 we present a family of $O(n,2)$ with a sub $O(n_2,2)$ by sum composition of an $O(n_1,2)$ based on $GF(n_1)$ and an arbitrary $O(n_2,2)$ where n_2 hits the upper bound namely $[n_1/2]$ where $[a]$ denotes the integer part of a . Section 7 presents a family of $O(n,2)$ with a sub $O(3,2)$ by sum composition of an $O(n_1,2)$ based on $GF(n_1)$ of odd order and an $O(3,2)$. Here 3 is the lowest order which n_2 can take on in our present theory (see also Section 10). In Section 8 we construct a family of $O(p^\alpha + 4,2)$ with sub $O(4,2)$. Section 9 concerns with the construction of a family of $O(p^\alpha + 5,2)$ with sub $O(5,2)$. The order of composed Latin squares in this case is always of the form $4t + 2$. Section 10 discusses the theory and indicates its extension in two different ways. Several unsolved problems are stated.

2. Preliminaries.

Let Σ be a set of cardinality $n \geq 1$. Let L be a Latin square of order n on Σ .

Definition 2.1. We say L has a transversal if there exists a collection of n cells in L with the properties that: (i) No row and column of L contains more than one cell of this collection, (ii) the entries of these cells exhaust the set Σ .

Of course not every Latin square has a transversal.

Definition 2.2. We say L has t parallel transversals if L contains t transversals no two of which have any cell in common.

Definition 2.3. Let L_1, L_2, \dots, L_r be r Latin squares of order n on Σ . Then a collection of n cells is said to form a common transversal for these r Latin squares if the collection is a transversal for each of these r Latin squares.

Definition 2.4. A set of r Latin squares of order n on Σ is said to contain t parallel common transversals if they have t common transversals which are pairwise parallel.

Hereafter, the symbol $O(n,r)$ denotes a set of r pairwise orthogonal Latin squares of order n . Also we use the notation of $L_1 \perp L_2$ to indicate that L_1 is orthogonal to L_2 . It is easy to see that:

Lemma 2.1. An $O(n,r)$ exists if and only if an $O(n,r-1)$ with n common parallel transversals exists.

Lemma 2.2. An $O(n,n-1)$ has no common transversal.

Example 2.1. Let $\Sigma = \{a,b,c,d\}$. Then the underlined and parenthesized cells form two common parallel transversals for the following $O(4,2)$.

(a)	b	<u>c</u>	d	(a)	c	<u>d</u>	b
c	(d)	a	<u>b</u>	b	(d)	e	<u>a</u>
<u>d</u>	c	(b)	a	<u>c</u>	a	(b)	d
b	<u>a</u>	d	(c)	d	<u>b</u>	a	(c)

3. Sum Composition of Latin Squares.

In order to make the reading of this paper independent of our previous papers [3], [4], [5], and [7] we shall review the sum composition technique for the construction of Latin squares of order $n_1 + n_2$ from Latin squares of orders n_1 and n_2 having certain combinatorial structures. Before proceeding further let us remark that sum composition has numerous applications:

(i) It can be used for the construction of Latin squares of order $n_1 + n_2$ with sub-Latin squares of order n_2 for all n_1 and $n_2 \leq n_1$ except for $(n_1, n_2) = (2,1), (2,2), (6,5)$ and $(6,6)$. (ii) It has an immediate application for the construction of pairs of orthogonal Latin squares of order $n_1 + n_2$, including those of the form $4t + 2$, with sub-orthogonal Latin squares of order n_2 . (iii) Latin squares and orthogonal Latin squares constructed via sum composition enjoy certain combinatorial properties which are useful for the construction of several useful experimental designs for successive

stages, see Hedayat, Parkes and Federer [6]. (iv) Hedayat [8] has utilized this method and has produced a Latin square of order 10 which is orthogonal to its transpose. Finally, Federer [2] has pointed out several other applications of sum composition.

In the sequel we need the following concepts: Consider an $m \times m$ square B having a Latin square L of order $n < m$ with a transversal in its $n \times n$ top left corner subsquare. By the vertical projection of a given transversal in L on the r -th row, $r > n$, of B we mean filling the (r, j) cell of this row by that element of the given transversal which appears in j -th column of L , $j = 1, 2, \dots, n$. Similarly by the horizontal projection of a given transversal on the t -th column, $t > n$, of B we mean filling the (i, t) cell of this column by that element of the given transversal which appears in the i -th row of L , $i = 1, 2, \dots, n$.

The following example clarifies the above concepts.

Example 3.1. Let L and B be the following squares.

$$L = \begin{array}{ccc} 1 & \underline{2} & 3 \\ 2 & 3 & \underline{1} \\ \underline{3} & 1 & 2 \end{array} \quad \text{and} \quad B = \begin{array}{|c|c|c|c|c|c|} \hline 1 & \underline{2} & 3 & & & \\ \hline 2 & 3 & \underline{1} & & & \\ \hline \underline{3} & 1 & 2 & & & \\ \hline & & & & & \\ \hline & & & & & \\ \hline & & & & & \\ \hline & & & & & \\ \hline \end{array}$$

The underlined cells form a transversal for L . The vertical and horizontal projections of this transversal on the 6th row and column of B produce the following square.

1	<u>2</u>	3		2	
2	3	<u>1</u>		1	
<u>3</u>	1	2		3	
3	2	1			

Now we are ready to describe the method of sum composition. Let Σ_1 and Σ_2 be two non-intersecting sets of cardinalities n_1 and n_2 respectively, $n_1 \geq n_2$. Let L_1 be a Latin square of order n_1 with n_2 parallel transversals on Σ_1 . Note that this is always possible except for $(n_1, n_2) = (2, 1), (2, 2), (6, 5)$ and $(6, 6)$. Let L_2 be a Latin square of order n_2 on Σ_2 . L_2 is not required to have any specific combinatorial structure. Let C_1 be an $m \times m$, $m = n_1 + n_2$, square containing L_1 and L_2 in the following fashion:

$$C_1 = \begin{array}{|c|c|} \hline L_1 & \\ \hline & L_2 \\ \hline \end{array} .$$

Project horizontally and vertically the n_2 transversals of L_1 on the last n_2 columns and rows of C_1 in any arbitrary manner. Note that we have $n_2!$ choices for the projections on the rows and $n_2!$ choices for the projections on the columns. Call the resulting square C_2 . Now replace the n_1 entries of each transversal by a fixed element of Σ_2 such that no two transversals are being replaced by the same element of Σ_2 . Call the resulting square L_3 . It is easy to see that the above process guarantees that L_3 is a Latin square of order $n_1 + n_2$ on $\Sigma_1 \cup \Sigma_2$.

The preceding steps can be elucidated via an example.

Example 3.2. Let $\Sigma_1 = \{1, 2, 3\}$, $\Sigma_2 = \{a, b\}$ and

$$L_1 = \begin{array}{ccc} \underline{1} & (2) & 3 \\ 2 & \underline{3} & (1) \\ (3) & 1 & \underline{2} \end{array} \quad \text{and} \quad L_2 = \begin{array}{cc} a & b \\ b & a \end{array} .$$

Note that the underlined and parenthesized cells form two parallel transversals for L_1 . Then

$$C_1 = \begin{array}{|c|c|c|c|c|} \hline \underline{1} & (2) & 3 & & \\ \hline 2 & \underline{3} & (1) & & \\ \hline (3) & 1 & \underline{2} & & \\ \hline & & & a & b \\ \hline & & & b & a \\ \hline \end{array} ,$$

and a possible

$$C_2 = \begin{array}{|c|c|c|c|c|} \hline \underline{1} & (2) & 3 & 2 & 1 \\ \hline 2 & \underline{3} & (1) & 1 & 3 \\ \hline (3) & 1 & \underline{2} & 3 & 2 \\ \hline 1 & 3 & 2 & a & b \\ \hline 3 & 2 & 1 & b & a \\ \hline \end{array} .$$

Observe that the underlined transversal has been projected on the fourth row and on the fifth column and the parenthesized transversal has been projected on the fifth row and on the fourth column. Now if we replace the entries of the underlined transversal by a and the parenthesized ones by b we obtain the following L_3 .

$$L_3 = \begin{array}{|c|c|c|c|c|} \hline a & b & 3 & 2 & 1 \\ \hline 2 & a & b & 1 & 3 \\ \hline b & 1 & a & 3 & 2 \\ \hline 1 & 3 & 2 & a & b \\ \hline 3 & 2 & 1 & b & a \\ \hline \end{array} .$$

4. Fundamental Lemmas in Sum Composition.

Let $\Sigma_1 = GF(n_1)$. Let $B(x)$ be a square of order n_1 with $x\alpha_i + \alpha_j$ in its (i,j) entry, $x \in GF(n_1)$, $x \neq 0$, $\alpha_i, \alpha_j \in GF(n_1)$. It is well known that $B[x]$ is a Latin square of order n_1 on Σ_1 and moreover

$$B(x) \perp B(y), x \neq y.$$

In particular $B(1)$, $B(x)$ and $B(y)$ form an $O(n_1, 3)$. Note that the n_1 entries in $B(x)$ and $B(y)$ corresponding to the n_1 entries equal to k , in $B(1)$, i.e., $\alpha_i + \alpha_j = k \in GF(n_1)$, form a common transversal for $B(x)$ and $B(y)$. We name this transversal by k . As k runs over all the elements of $GF(n_1)$ we obtain n_1 common transversals for $B(x)$ and $B(y)$. Moreover, two common transversals k and ℓ , $k \neq \ell$ are parallel. Thus we have located and named n_1 common parallel transversals in $B(x)$ and $B(y)$.

Consider the following two $n \times n$, $n = n_1 + n_2$, $n_2 \leq n_1$ squares

$$C(x) = \begin{array}{|c|c|} \hline B(x) & \\ \hline & \\ \hline \end{array} \quad C(y) = \begin{array}{|c|c|} \hline B(y) & \\ \hline & \\ \hline \end{array}.$$

Project the transversal s in $B(x)$ vertically and horizontally on an arbitrary row and column of $C(x)$. Call the resulting square $C'(x)$. Project also the transversal t in $B(y)$ vertically and horizontally on the same row and column numbers of $C(y)$. Call the resulting square $C'(y)$. The following two lemmas characterize the $2n_1$ ordered pairs obtained upon superposition of $C'(x)$ on $C'(y)$ corresponding to the projected transversals s and t .

Lemma 4.1. The set of n_1 ordered pairs resulted from the superposition of the vertical projection of the transversal s in $B(x)$ and transversal t in $B(y)$ forms the same set of ordered pairs as obtained by superposition of the transversal $k_v(x, y, s, t)$ in $B(x)$ and in $B(y)$ for

$$(4.1) \quad k_v(x, y, s, t) = [sx(1-y) - ty(1-x)]/(x-y), x \neq y.$$

Proof. The entries of the transversal s in $B(x)$ and the transversal t in $B(y)$ respectively reads

$$\begin{aligned} x\alpha_i + \alpha_j, \alpha_i + \alpha_j &= s \\ y\alpha_i^* + \alpha_j^*, \alpha_i^* + \alpha_j^* &= t. \end{aligned}$$

Upon vertical projection of these transversals the n_1 entries respectively read as

$$x(s - \alpha_j) + \alpha_j \quad \text{and} \quad y(t - \alpha_j) + \alpha_j .$$

Therefore upon superposition of these projected transversals we obtain the n_1 pairs

$$(4.2) \quad (x(s - \alpha_j) + \alpha_j, y(t - \alpha_j) + \alpha_j), \quad j = 1, 2, \dots, n_1 .$$

Now let α'_i and α'_j be such that

$$k_v(x, y, s, t) = \alpha'_i + \alpha'_j .$$

Upon superposition of transversal $k_v(x, y, s, t)$ in $B(x)$ and $B(y)$ we obtain the following n_1 pairs

$$(4.3) \quad (x\alpha'_i + \alpha'_j, y\alpha'_i + \alpha'_j) .$$

Equating (4.2) to (4.3) results in

$$\begin{aligned} x(s - \alpha_j) + \alpha_j &= x\alpha'_i + \alpha'_j \\ y(t - \alpha_j) + \alpha_j &= y\alpha'_i + \alpha'_j \end{aligned}$$

which yields the following solution for $k_v(x, y, s, t)$.

$$k_v(x, y, s, t) = [sx(1-y) - ty(1-x)]/(x-y) \quad \text{Q.E.D.}$$

Note that if in particular $x = y^{-1}$ we obtain the following simple expression for $k_v(y^{-1}, y, s, t)$.

$$(4.4) \quad k_v(y^{-1}, y, s, t) = (ty + s)/(1+y),$$

which will be denoted by $k_v(y, s, t)$ for simplicity.

Lemma 4.2. The set of n_1 ordered pairs resulted from the superposition of the horizontal projection of the transversal s in $B(x)$ and transversal t in $B(y)$ forms the same set of ordered pairs as obtained by superposition of the transversal $k_h(x,y,s,t)$ in $B(x)$ and in $B(y)$ for

$$(4.5) \quad k_h(x,y,s,t) = [t(x-1) - s(y-1)]/(x-y), \quad x \neq y.$$

The proof is analogous to the proof of Lemma 4.1.

If in particular $x = y^{-1}$ the expression (4.5) reduces to the following simple expression

$$(4.6) \quad k_h(y^{-1},y,s,t) = (sy + t)/(1+y),$$

which will be denoted by $k_h(y,s,t)$ for simplicity.

Remark 4.1.

$$(4.7) \quad k_v(x,y,s,t) + k_h(x,y,s,t) = (t+s) + \frac{(t-s)(xy-1)}{(x-y)} = s+t \quad \text{if } x = y^{-1}.$$

Remark 4.2. To simplify the detailed descriptions of Lemmas 4.1 and 4.2 henceforth we refer to them in the following forms:

(i) The vertical projection of the transversal s in $B(x)$ and the transversal t in $B(y)$ will jointly capture the transversal $k_v(x,y,s,t)$ as given in (4.1).

(ii) The horizontal projection of the transversal s in $B(x)$ and the transversal t in $B(y)$ will jointly capture the transversal $k_h(x,y,s,t)$ as given in (4.5).

5. An Application of Sum Composition for the Construction of Sets of Orthogonal Latin Squares.

In order to construct an $O(n,2)$ for $n = n_1 + n_2$, we require that $n_1 \geq 2n_2$ and there should exist an $O(n_2,2)$ and an $O(n_1,2)$ with $2n_2$ common parallel transversals. In this section, due to some combinatorial

difficulties, we exclude the case $n_2 = 1$ even though an $O(1,2)$ exists. The above requirements eliminate the arbitrary decomposition of n into n_1 and n_2 . For instance we should exclude $n_2 = 2$ or 6 . Thus the range of n_2 is $3 \leq n_2 \leq \lfloor n_1/2 \rfloor$. The following lemma guarantees that for any $n \geq 10$ there is at least one decomposition of n which fulfill the preceding requirements.

Lemma 5.1. For any $n \geq 10$ there exists a decomposition $n = n_1 + n_2$ with the property that the existence of an $O(n_2, 2)$ and an $O(n_1, 2)$ with at least $2n_2$ common parallel transversals are guaranteed.

Proof. It is a well known fact in number theory that any $n \geq 10$ can be decomposed into $n_1 + n_2$, $n_1 = p^\alpha$, p a prime and α a positive integer, $n_1 \geq 2n_2$, $n_2 \geq 3$, $n_2 \neq 6$. It is also well known that for any $n_1 = p^\alpha$ there is an $O(n_1, n_1 - 1)$. These together with the fact that for any $n_2 = 2, 6$ there is an $O(n_2, 2)$ complete the proof.

Now let $n = n_1 + n_2$, $n \geq 10$, $n_1 = p^\alpha$, $n_2 \geq 3$, $n_2 \neq 6$ and $n_1 \geq 2n_2$. Let $B(x)$ and $B(y)$, $x \neq 1$, $y \neq 1$, $x \neq y$, be two Latin squares of order n_1 on $\Sigma_1 = GF(n_1)$. Let also $\{A_1, A_2\}$ be an $O(n_2, 2)$ on Σ_2 of cardinality n_2 such that $\Sigma_1 \cap \Sigma_2 = \emptyset$. Let Ω be a set of $2n_2$ parallel transversals for $\{B(x), B(y)\}$. Note that Ω can be constructed in $\binom{n_1}{2n_2}$ different ways. Decompose Ω into two nonintersecting sets S and T each of cardinality n_2 . Let L_1 be any Latin square of order $n_1 + n_2$ captured by sum composition of $B(x)$ and A_1 using the transversals in S (see Section 3). Let L_2 be any Latin square of order $n_1 + n_2$ constructed by sum composition of $B(y)$ and A_2 using the transversals in T . The following lemma constitutes the backbone for the remainder of this section.

Lemma 5.2. $\{L_1, L_2\}$ is an $O(n, 2)$ if $K_v \cup K_h = \Omega$, where K_v and K_h denote the sets of captured transversals on rows and columns respectively.

Proof. Upon superposition of L_1 on L_2 the following is true:

- (i) Every element of Σ_2 in L_1 appears with every other element of Σ_2 in L_2 , due to the fact that $A_1 \perp A_2$ in the lower right corner.
- (ii) Every element of Σ_2 in L_1 appears with every element of Σ_1 in L_2 because we have replaced the entries of the transversals in S by the elements of Σ_2 .
- (iii) Every element of Σ_1 in L_1 appears with every element of Σ_2 in L_2 because the entries of the transversals in T have been replaced by the elements of Σ_2 .

Therefore, all we have to prove is that every element of Σ_1 in L_1 appears with every other element of Σ_1 in L_2 . To prove this recall that $B(x) \perp B(y)$. However, since we removed the n_2 transversals in $B(x)$ determined by the n_2 elements of S and n_2 transversals in $B(y)$ determined by the n_2 elements of T therefore the following $2n_2n_1$ pairs have been lost.

$$(x\alpha_i + \alpha_j, y\alpha_i + \alpha_j) \text{ with } \alpha_i + \alpha_j = \gamma \in \Omega.$$

But the condition of the lemma guarantees the capture of these lost pairs by the $2n_2n_1$ bordered cells. Q.E.D.

The following example elucidates Lemma 5.1.

Example 5.1. Let $n = 10 = 7 + 3$ with

$$\Sigma_1 = \text{GF}(7) = \{0, 1, 2, 3, 4, 5, 6\} \text{ and } \Sigma_2 = \{7, 8, 9\}.$$

Set $x = 2, y = 5$. Then

$$B(2) = \begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \end{array}, \quad B(5) = \begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \end{array}.$$

In order to locate the common parallel transversals in $B(x)$ and $B(y)$ we exhibit here the $B(1)$.

$$B(1) = \begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \end{array} .$$

Let also

$$A_1 = \begin{array}{ccc} 7 & 8 & 9 \\ 8 & 9 & 7 \\ 9 & 7 & 8 \end{array} , \quad A_2 = \begin{array}{ccc} 7 & 8 & 9 \\ 9 & 7 & 8 \\ 8 & 9 & 7 \end{array} .$$

We select $\Omega = \{0,1,2,3,4,5\}$ and $\Omega = S \cup T = \{0,1,3\} \cup \{2,4,5\}$. Now notice that for the following pairing of s 's and t 's we have

$$\begin{aligned} k_v(x,y,s,t) = k_v(2,5,s,t) &= 5 \text{ for } s = 0, t = 4, \\ &= 4 \text{ for } s = 1, t = 2, \\ &= 2 \text{ for } s = 3, t = 5, \end{aligned}$$

and

$$\begin{aligned} k_h(x,y,s,t) = k_h(2,5,s,t) &= 1 \text{ for } s = 0, t = 4, \\ &= 3 \text{ for } s = 1, t = 2, \\ &= 0 \text{ for } s = 3, t = 5 . \end{aligned}$$

Therefore for these pairings $K_v = \{5,4,2\}$ and $K_h = \{1,3,0\}$ and thus $K_v \cup K_h = \Omega$. We remark that here $K_v = T$ and $K_h = S$. But in general there is no such requirement.

Now we assemble all the parts to get L_1 and L_2 as follows:

$L_1 =$	7	8	2	9	4	5	6	0	1	3
	8	3	9	5	6	0	7	1	2	4
	4	9	6	0	1	7	8	2	3	5
	9	0	1	2	7	8	5	3	4	6
	1	2	3	7	8	6	9	4	5	0
	3	4	7	8	0	9	2	5	6	1
	5	7	8	1	9	3	4	6	0	2
	0	6	5	4	3	2	1	7	8	9
	2	1	0	6	5	4	3	8	9	7
	6	5	4	3	2	1	0	9	7	8

and $L_2 =$

0	1	9	3	7	8	6	4	2	5
5	9	0	7	8	3	4	1	6	2
9	4	7	8	0	1	2	5	3	6
1	7	8	4	5	6	9	2	0	3
7	8	1	2	3	9	5	6	4	0
8	5	6	0	9	2	7	3	1	4
2	3	4	9	6	7	8	0	5	1
6	2	5	1	4	0	3	7	8	9
3	6	2	5	1	4	0	9	7	8
4	0	3	6	2	5	1	8	9	7

The reader can satisfy his curiosity by direct checking that L_1 and L_2 is a pair of orthogonal Latin squares of order 10.

Remark 5.1. The major problem with regard to the construction of an $O(n,2)$ via sum composition is the following:

- (i) How to choose x and y . We have found that $y = x^{-1}$ simplifies the calculations considerably.
- (ii) How to select the set Ω from the $\binom{n_1}{2n_2}$ possible choices.
- (iii) How to split Ω into $S \cup T$.
- (iv) In the formation of L_1 and L_2 how should we project (vertically and horizontally) the members of S and T , if possible, so that

$$K_v \cup K_h = \Omega.$$

We found that the backward solution of the problem, especially in the case $y = x^{-1}$, is easier. Namely, devise any "admissible scheme" of capturing the members of Ω via vertical or horizontal projections. Here by an "admissible scheme" we mean we should never let

$$k_v(x,y,s,t) = s \text{ or } t$$

or

$$k_h(x,y,s,t) = s \text{ or } t,$$

since it is impossible to capture s or t through the pair (s,t) . Then the problem reduces to solving a system of $2n_2$ homogenous equations in

$2n_2$ unknowns. The entries of the related matrix are in terms of x and y . Now the question is this. For what x and y and in what finite field this system has a nontrivial solution with distinct components. Summing up the $2n_2$ equations we obtain $(\sum s_i - \sum t_i) \left(\frac{1-xy}{x-1} \right) = 0$. This equation is independent of either the value of n_2 or the finite field in which the equations are supposed to hold. Thus our system of equations will have no trivial solutions provided that either $xy = 1$ or $\sum s_i = \sum t_i$. This justifies further the relation $xy = 1$ used in our investigations to simplify the calculations. However $xy = 1$ does not yet solve our problem. We are searching for solution with distinct components. This lead in our investigations to the reduction of the rank to $2n_2 - 2$ and consequently to a condition that y has to be a root of some polynomial. Whenever the polynomial was of degree two we could characterize easily the finite fields in which the components of the solutions are distinct. We got into difficulties when y had to be a root of a polynomial of degree higher than two since there are no readily available tools to characterize such fields.

6. Construction of Families of $O(n_1 + n_2, 2)$ With the Maximum Value of n_2 .

As we mentioned in Section 5 the maximum value that n_2 can take is $[n_1/2]$. We shall now present a family of $O(n, 2)$, $n = n_1 + n_2$ where n_2 takes its maximum value.

Theorem 6.1. For any prime p and any positive integer α such that $n_1 = p^\alpha \geq 7$, $n_1 \neq 13$, one can construct an $O(n, 2)$ with the sum composition of an $O(n_1, 2)$ based on $GF(n_1)$ and any $O(n_2, 2)$ where $n_2 = [n_1/2]$.

Proof. By construction. Let $\Sigma_1 = GF(n_1)$ and Σ_2 any set of cardinality n_2 such that $\Sigma_1 \cap \Sigma_2 = \emptyset$. Let $\{B(x), B(y)\}$ be an $O(n_1, 2)$ based on $GF(n_1)$ and $\{A_1, A_2\}$ any $O(n_2, 2)$ based on Σ_2 . Let $\lambda \in GF(n_1)$, $\lambda \neq 0$ if n_1 is even. Let also $\Omega = GF(n_1) - \{\lambda\} = S \cup T$ such that for any $s \in S$ there is $t \in T$ such that $s + t = \lambda$. Construct a Latin square L_1

by the sum composition of $B(x)$ and A_1 using any arbitrary vertical and horizontal projections of the n_2 parallel transversals determined by the elements of S . Now construct the Latin square L_2 by the sum composition of $B(y)$ and A_2 using the n_2 transversals in $B(y)$ determined by the elements of T and the following projection rules: Project transversal t_i on the row (column) which upon superposition of L_2 on L_1 this row (column) should fall on the row (column) stemmed from the transversal $s_i = \lambda - t_i$. Now by (4.7)

$$k_v(y, s, t) + k_h(y, s, t) = (s+t) + (t-s)(xy-1)/(x-y),$$

therefore if we set $x = y^{-1}$ then for $s_1 \neq s_2$ we have $k_v(y, s_1, \lambda - s_1) \neq k_v(y, s_2, \lambda - s_2)$ and $k_h(y, s_1, \lambda - s_1) \neq k_h(y, s_2, \lambda - s_2)$. This implies that $K_v \cup K_h$ has cardinality $n_1 - 1$ and $K_v \cup K_h = \Omega$ and thus by Lemma 5.2 the set $\{L_1, L_2\}$ is an $O(n, 2)$ on $\Sigma_1 \cup \Sigma_2$.

Remark. The method of Theorem 6.1 fails for $n_1 = 13$ only because there is no $O(6, 2)$. Otherwise, there will be no orthogonality contradiction on the other parts of L_1 and L_2 with their 6×6 lower right corner missing.

Corollary 6.1. The method of Theorem 6.1 produces infinitely many pairs of orthogonal Latin squares of order $4t+2$.

Proof. Let $p \equiv 7 \pmod{8}$ and α odd, then $p^\alpha = (8t+5)/3$ and thus $n_1 + n_2 = 4t+2$.

Corollary 6.2. If $p^\alpha > 7$, then the composed orthogonal Latin squares in Theorem 6.1 has at least one common transversal if the corner $O(n_2, 2)$ has a common transversal.

Proof. The original $O(p^\alpha, 2)$ has p^α common parallel transversals. Therefore after removing $p^\alpha - 1$ common parallel transversals we are left with one common transversal in the corresponding portion of $O(p^\alpha, 2)$ in the composed $O(n, 2)$. This common transversal together with the assumed common

transversal in the lower right corner $O(n_2, 2)$ form a common transversal for the composed $O(n, 2)$. The reason for the exclusion of $p^\alpha = 7$ is the fact that no $O(3, 2)$ with common transversal exists (see Lemma 2.2).

$O(n, 2)$ with common parallel transversals have an application for the construction of a family of designs for two successive experiments (see Hedayat, Parker and Federer [6]).

We shall now clarify the method of Theorem 6.1 by two examples, one for n_1 odd and one for n_1 even.

Example 6.1. Let $n_1 = 7$, $GF(7) = \{0, 1, \dots, 6\}$. Then for $y = 3$, $x = y^{-1} = 5$ we have $\{B(1), B(5), B(3)\} =$

0 1 2 3 4 5 6	0 1 2 3 4 5 6	0 1 2 3 4 5 6
1 2 3 4 5 6 0	5 6 0 1 2 3 4	3 4 5 6 0 1 2
2 3 4 5 6 0 1	3 4 5 6 0 1 2	6 0 1 2 3 4 5
3 4 5 6 0 1 2	1 2 3 4 5 6 0	2 3 4 5 6 0 1
4 5 6 0 1 2 3	6 0 1 2 3 4 5	5 6 0 1 2 3 4
5 6 0 1 2 3 4	4 5 6 0 1 2 3	1 2 3 4 5 6 0
6 0 1 2 3 4 5	2 3 4 5 6 0 1	4 5 6 0 1 2 3

For $n_2 = (n_1 - 1)/2$ let $\Sigma_2 = \{7, 8, 9\}$ and

$$\{A_1, A_2\} = \begin{array}{cc} 7 & 8 & 9 \\ 8 & 9 & 7 \\ 9 & 7 & 8 \end{array}, \begin{array}{cc} 7 & 8 & 9 \\ 9 & 7 & 8 \\ 8 & 9 & 7 \end{array}.$$

Finally for $\lambda = 1$, $S = \{1, 2, 3\}$ and $T = \{0, 6, 5\}$ we have $\{L_1, L_2\} =$

0 7 8 9 4 5 6	1 2 3	7 1 2 3 4 9 8	0 6 5
7 8 9 1 2 3 4	5 6 0	3 4 5 6 9 8 7	2 1 0
8 9 5 6 0 1 7	2 3 4	6 0 1 9 8 7 5	4 3 2
9 2 3 4 5 7 8	6 0 1	2 3 9 8 7 0 1	6 5 4
6 0 1 2 7 8 9	3 4 5	5 9 8 7 2 3 4	1 0 6
4 5 6 7 8 9 3	0 1 2	9 8 7 4 5 6 0	3 2 1
<u>2 3 7 8 9 0 1</u>	<u>4 5 6</u>	<u>8 7 6 0 1 2 9</u>	<u>5 4 3</u>
5 1 4 0 3 6 2	7 8 9	0 5 3 1 6 4 2	7 8 9
3 6 2 5 1 4 0	8 9 7	4 2 0 5 3 1 6	9 7 8
1 4 0 3 6 2 5	9 7 8	1 6 4 2 0 5 3	8 9 7

which is an $O(10,2)$.

Example 6.2. Let $n_1 = 8$, $GF(8) = \{0,1,\dots,7\}$ with the following addition (+) and multiplication (x) tables:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	6	4	3	7	2	5
2	2	6	0	7	5	4	1	3
3	3	4	7	0	1	6	5	2
4	4	3	5	1	0	2	7	6
5	5	7	4	6	2	0	3	1
6	6	2	1	5	7	3	0	4
7	7	5	3	2	6	1	4	0

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	3	4	5	6	7	1
3	0	3	4	5	6	7	1	2
4	0	4	5	6	7	1	2	3
5	0	5	6	7	1	2	3	4
6	0	6	7	1	2	3	4	5
7	0	7	1	2	3	4	5	6

Then for $y = 3$, $x = y^{-1} = 6$ we have $\{B(1), B(6), B(3)\} =$

0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
1 0 6 4 3 7 2 5	6 2 1 5 7 3 0 4	3 4 7 0 1 6 5 2
2 6 0 7 5 4 1 3	7 5 3 2 6 1 4 0	4 3 5 1 0 2 7 6
3 4 7 0 1 6 5 2	1 0 6 4 3 7 2 5	5 7 4 6 2 0 3 1
4 3 5 1 0 2 7 6	2 6 0 7 5 4 1 3	6 2 1 5 7 3 0 4
5 7 4 6 2 0 3 1	3 4 7 0 1 6 5 2	7 5 3 2 6 1 4 0
6 2 1 5 7 3 0 4	4 3 5 1 0 2 7 6	1 0 6 4 3 7 2 5
7 5 3 2 6 1 4 0	5 7 4 6 2 0 3 1	2 6 0 7 5 4 1 3

For $n_2 = n_1/2 = 4$, let $\Sigma_2 = \{A,B,C,D\}$ and

$$\{A_1, A_2\} = \begin{array}{cc} \begin{array}{cccc} A & B & C & D \\ B & A & D & C \\ C & D & A & B \\ D & C & B & A \end{array} & , \quad \begin{array}{cccc} A & B & C & D \\ C & D & A & B \\ D & C & B & A \\ B & A & D & C \end{array} \end{array} .$$

Finally for $\lambda = 2$, $S = \{0,1,3,4\}$ and $T = \{2,6,7,5\}$ we have $\{L_1, L_2\} =$

A	B	2	C	D	5	6	7	0	1	3	4
B	A	1	D	C	3	0	4	2	6	7	5
7	5	A	2	6	D	B	C	3	4	0	1
C	D	6	A	B	7	2	5	4	3	1	0
D	C	0	B	A	4	1	3	5	7	6	2
3	4	D	0	1	A	C	B	6	2	5	7
4	3	B	1	0	C	A	D	7	5	2	6
5	7	C	6	2	B	D	A	1	0	4	3
0	2	3	4	5	6	7	1	A	B	C	D
6	1	5	7	3	0	4	2	B	A	D	C
1	6	4	3	7	2	5	0	C	D	A	B
2	0	7	5	4	1	3	6	D	C	B	A

0	1	A	3	4	D	B	C	2	6	7	5
3	4	B	0	1	C	A	D	5	7	6	2
A	B	5	C	D	2	7	6	4	3	1	0
5	7	C	6	2	B	D	A	1	0	4	3
6	2	D	5	7	A	C	B	3	4	0	1
D	C	3	B	A	1	4	0	6	2	5	7
B	A	6	D	C	7	2	5	0	1	3	4
C	D	0	A	B	4	1	3	7	5	2	6
4	0	2	7	6	3	5	1	A	B	C	D
1	3	7	2	5	0	6	4	C	D	A	B
2	5	4	1	3	6	0	7	D	C	B	A
7	6	1	4	0	5	3	2	B	A	D	C

which is an $O(12,2)$.

7. Construction of Families of $O(n_1 + n_2, 2)$ With the Minimum Value of n_2 .

Presently we shall investigate the problem of construction of a set $O(n, 2)$ for $n = n_1 + 3$, $n_1 = p^\alpha$, p a prime greater or equal to seven and α a positive integer. It is clearly enough to show that the construction can be achieved for any $p \geq 7$. It then can be carried over to any $n_1 = p^\alpha$.

As before let $B(1)$, $B(x)$ and $B(y)$ be three orthogonal Latin squares with elements in $GF(n_1)$.

Let $S = \{s_1, s_2, s_3\}$, $T = \{t_1, t_2, t_3\}$ denote sets of transversals projected from $B(x)$ and $B(y)$ respectively.

The problem faced now is, can one choose the sets S and T in such a manner that the ranges of the two functions $k_v(x, y, s, t_j)$ and $k_h(x, y, s_i, t_j)$ for $i, j = 1, 2, 3$ exhaust the sets $S \cup T$ and if so in what way, if any, does the choice depend on x and y . This leads to the problem, how many distinct systems of choices are at all possible. Reducing the problem to nonisomorphic cases we shall consider two cases distinct if they cannot be obtained from each other by interchanging the squares transposing both squares or permuting the elements within each of the sets S or T . Thus we may assume that for one of the functions, say $k_v(x, y, s_i, t_j)$, $i = j$, since this can be achieved by permuting the elements of one of the sets S or T . Furthermore we shall assume that the range of the function $k_v(x, y, s_i, t_i)$ consists of either two or three elements of the set S . Cases in which the range includes none or one element of S can be obtained from the above by interchanging the sets S and T and the functions k_v and k_h . To facilitate the notation we shall omit the arguments x and y in present considerations.

It is easy to see, in view of the above, that there are just four distinct patterns for the range of $k_v(s, t)$. They are:

I	II	III	IV
$k_v(s_1, t_1) = s_2$	$k_v(s_1, t_1) = s_2$	$k_v(s_1, t_1) = s_2$	$k_v(s_1, t_1) = s_2$
$k_v(s_2, t_2) = s_3$	$k_v(s_2, t_2) = s_3$	$k_v(s_2, t_2) = s_3$	$k_v(s_2, t_2) = s_1$
$k_v(s_3, t_3) = s_1$	$k_v(s_3, t_3) = t_1$	$k_v(s_3, t_3) = t_2$	$k_v(s_3, t_3) = t_1$.

For each of these patterns there are twelve distinct possibilities for the range of $k_h(s_i, t_j)$. Thus there are in total 48 cases to be considered.

In our previous work (1971) we assumed that $xy = 1$. This seemed to simplify the calculations. We hoped that such a restriction will not play

an essential role in obtaining the results we aimed at. Ruiz and Seiden (1972) showed that a necessary and sufficient condition for obtaining non trivial solutions for the systems of equations arising in the method of sum composition is either $\sum s_i = \sum t_i$ or $xy = 1$. They also showed that for patterns II, III and IV the elements of $S \cup T$ cannot be distinct unless $xy = 1$.

We shall show here that under the assumption $xy = 1$ one cannot construct a set $O(n_1 + 3, 2)$ for some primes n_1 , of the form $60m + 11$ and $60m + 59$. However using pattern I and another relation between x and y we shall be able to bridge this gap.

We investigated fully all 48 distinct systems of equations under the assumption $xy = 1$. This reduced, as mentioned before, the rank of the system to at most five. However imposing in addition the condition that the solutions must be distinct reduced the rank in all cases to at most four and yielded a condition that y must be a root of certain equations. There were cases in which y had to satisfy either the equation $y = 0$ or $y = 1$. Clearly this was incompatible with the condition $xy = 1, x \neq y$. In other cases the problem reduced to solving either a quadratic or a fourth degree equation in y in Galois fields. The cases of quadratic equations were easily analyzed. The latter helped to establish that if $xy = 1$ there are primes for which a set $O(n_1 + 3, 2)$ cannot be constructed.

The cases in which y had to be a root of quadratic equation separated the primes for which a set $O(n_1 + 3, 2)$ could be constructed into four classes not necessarily disjoint. They were such that either $-1, -2, -3$, or -15 are quadratic residues in $GF(n_1)$. We shall present now a representative pattern for each of these classes

<u>Case 1.</u>	$k_v(s_1, t_1) = s_2$	$k_h(s_1, t_2) = t_1$	
	$k_v(s_2, t_2) = s_3$	$k_h(s_2, t_1) = t_3$.
	$k_v(s_3, t_3) = s_1$	$k_h(s_3, t_3) = t_2$	

This system will be of rank four and exhaust the elements of the set $S \cup T$ provided that y is a root of the equation $2y^2 + 3y + 3 = 0$. Hence

$y = \frac{-3 \pm \sqrt{-15}}{4}$ and the system will have solutions provided that either -3 and 5 or -5 and 3 are quadratic residues mod p .

A system of solutions is:

$$s_1 = (y^2 + y + 1)s_2 - y(y+1)t_2$$

$$t_1 = -ys_2 + (y + 1)t_2$$

$$s_3 = s_2/(y + 1) + yt_2/(y+1)$$

$$t_3 = (y^3 + y^2 + y)s_2/(y + 1) - (y^3 + y^2 - 1)/(y + 1) .$$

Case 2. $k_v(s_1, t_1) = s_2$

$$k_h(s_1, t_2) = t_3$$

$$k_v(s_2, t_2) = s_3$$

$$k_h(s_2, t_1) = s_1$$

$$k_v(s_3, t_3) = t_1$$

$$k_h(s_3, t_3) = t_2 .$$

For this system to be solvable and exhaust the set $S \cup T$, y has to be a root of the equation $y^2 + y + 1 = 0$, i.e., -3 has to be quadratic residue or p of the form $6m + 1$. The following forms a system of solutions:

$$s_1 = -s_3/(y + 1) + (y + 2)t_3/(y + 1)$$

$$s_2 = (2y + 1)s_3/(y + 1) - yt_3/(y + 1)$$

$$t_1 = s_3/(y + 1) + yt_3/(y + 1)$$

$$t_2 = ys_3/(y + 1) + t_3/(y + 1) .$$

Case 3. $k_v(s_1, t_1) = s_2$

$$k_h(s_1, t_1) = t_3$$

$$k_v(s_2, t_2) = s_3$$

$$k_h(s_2, t_2) = s_1$$

$$k_v(s_3, t_3) = t_1$$

$$k_h(s_3, t_3) = t_2 .$$

This system will be of rank four and the solutions will exhaust the set $S \cup T$ provided that y is a root of the equation $2y^2 + 1 = 0$, i.e., -2 is a quadratic residue or $p = 8m + 1$ or $8m + 3$.

A system of solutions is:

$$\begin{aligned} s_3 &= ys_1 + (1 - y)s_2 \\ t_1 &= 2ys_1 - (2y - 1)s_2 \\ t_2 &= (1 + y)s_1 - ys_2 \\ t_3 &= (1 + 2y)s_1 - 2ys_2 \end{aligned}$$

Case 4.

$$\begin{aligned} k_v(s_1, t_1) &= s_2 & k_h(s_1, t_1) &= t_3 \\ k_v(s_2, t_2) &= s_3 & k_h(s_2, t_3) &= s_1 \\ k_v(s_3, t_3) &= t_2 & k_h(s_3, t_2) &= t_1 \end{aligned}$$

This system will be of rank four and exhaust the set $S \cup T$ provided that $y^2 + 1 = 0$, i.e., -1 has to be a quadratic residue or $p = 4m + 1$.

A system of solution is:

$$\begin{aligned} s_2 &= s_1/(y+1) + yt_1/(y+1) & t_2 &= -s_1/(y+1) - (y^2 - y - 1)t_1/(y+1) \\ s_3 &= s_1/y(y+1) + (2y+1)t_1/(y+1) & t_3 &= ys_1/(y+1) + yt_1/(y+1) \end{aligned}$$

Since case 4 captures all primes of the form $4m + 1$ the problem is are they primes of the form $4m + 3$ which are not captured by the remaining three cases. Case 3 captures all primes of the form $4m + 3$ for m even. Case 2 will capture primes of the form $4m + 3$ for m odd, only provided that they are also of the form $6m + 1$. Hence cases 2, 3 and 4 left out primes of the form $12m + 11$ for m odd. Case 1 captures two families of these primes, provided that they are also of the form $60m + 23 = 12(5m + 1) + 11$ or $60m + 47 = 12(5m + 3) + 11$. Thus none of the four cases captured primes of the form $12(5m + 2) + 11$ and $12(5m + 4) + 11$.

The next question we asked was whether the failure to capture the above mentioned primes was due to the restriction $xy = 1$. Could we assuming

$xy \neq 1$ but $\sum s_i = \sum t_i$ supplement the missing primes? We shall show that the answer is in the affirmative.

We shall show that keeping the assumption $xy = 1$, we may capture some but not all of the missing primes. As mentioned before some of the 48 patterns lead to conditions that y has to satisfy a fourth degree equation. There were five equations of degree four as follows:

1. $y^4 + 2y^3 + 3y^2 + y + 1 = 0$
2. $y^4 + 2y^3 + 3y^2 + 3y + 2 = 0$
3. $y^4 + 3y^3 + 6y^2 + 5y + 2 = 0$
4. $y^4 + 2y^3 + 4y^2 + 4y + 2 = 0$
5. $y^4 + 3y^3 + 6y^2 + 6y + 3 = 0$.

It is easy to show that equations 4 and 5 cannot have a linear factor unless p is of the form $6m + 1$ or $4m + 1$ respectively. Hence these patterns cannot yield primes not obtainable otherwise. It also can be seen that the set of primes which can be captured by equations 1 and 2 are identical. Hence the problem reduces to investigating one of the first two equations and equation 3. Using the high speed computer facilities at Michigan State University we found that some but not all of the missing primes of the form $60m + 11$ and $60m + 59$ can be captured by these equations.

We investigated the first 10 primes of the two missing types of primes and found that in $GF(191)$ and $GF(1319)$ both equations did not have a linear factor and each of these primes is the smallest in its class.

It may be worthwhile mentioning that the number of solutions in the cases investigated was the same for both equations. We suspect that this holds for all finite fields but we lack the tools to investigate the problem. We would like to have a method to characterize finite fields in which equations of degree greater than two have roots. This would prove very useful for our further research on sum composition.

Let us assume now $xy \neq 1$ but $\sum s_i = \sum t_i$. We shall apply this assumption to pattern I since, as mentioned before, for patterns II through IV $xy = 1$ is a necessary condition. It will be shown that the choice $(1-x)/(x-y) = 1$ will prove sufficient to capture the missing primes. Writing now case I in terms of x we obtain:

$$\begin{aligned} s_1 &= 2xs_3 - (2x-1)t_3 & t_1 &= 2s_1 - t_2 \\ s_2 &= 2xs_1 - (2x-1)t_2 & t_3 &= 2s_2 - t_1 \\ s_3 &= 2xs_2 - (2x-1)t_2 & t_2 &= 2s_3 - t_3 \end{aligned}$$

This system will have rank four and yield distinct solutions for the unknowns provided that x satisfies the equation $4x^2 - 6x + 1 = 0$. Hence $x = (3 \pm \sqrt{5})/4$. Thus this system will capture all primes n_1 such that 5 is a quadratic residue in $GF(n_1)$, i.e. n_1 is of the form $5m + 1$ or $5m + 4$. Primes of the form $5m + 1$ and $5m + 4$ include primes of the form $60m + 11$ and $60m + 59$ respectively.

A system of solution is:

$$\begin{aligned} s_1 &= 2xs_3 - (2x-1)t_3 \\ t_2 &= 2s_3 - t_3 \\ t_1 &= 2(2x-1)s_3 - (4x-3)t_3 \\ s_2 &= (2x-1)s_3 - 2(x-1)t_3 \end{aligned}$$

We are ready now to summarize the result of the previous discussion in the following theorem.

Theorem 7.1. Using the method of sum composition it is possible to construct a set $O(p^\alpha + 3, 2)$ for all $p \geq 7$.

We remind the reader that the method of construction depends on the form of p but not on its specific value.

Corollary 7.1. The method of Theorem 7.1 produces an infinite family of $O(n, 2)$ with $n = 4t + 2$.

Example 7.1. Let us construct a pair of orthogonal Latin squares of order 14 by sum composition of an $O(11,2)$ and an $O(3,2)$. Utilizing case 3 we obtain $y = 4, x = 3, S = \{0,1,8\}$ and $T = \{4,7,3\}$ and finally the following $O(14,2)$.

A	E	2	3	4	5	6	7	C	9	10	0	1	8	0	1	2	A	B	5	6	C	8	9	10	4	7	3
B	4	5	6	7	8	9	C	0	1	A	2	3	10	4	5	A	B	8	9	C	0	1	2	3	7	10	6
6	7	8	9	10	0	C	2	3	A	B	4	5	1	8	A	B	0	1	C	3	4	5	6	7	10	2	9
9	10	0	1	2	C	4	5	A	B	8	6	7	3	A	B	3	4	C	6	7	8	9	10	0	2	5	1
1	2	3	4	C	6	7	A	B	10	0	8	9	5	B	6	7	C	9	10	0	1	2	3	A	5	8	4
4	5	6	C	8	9	A	B	1	2	3	10	0	7	9	10	C	1	2	3	4	5	6	A	B	8	0	7
7	8	C	10	0	A	B	3	4	5	6	1	2	9	2	C	4	5	6	7	8	9	A	B	1	0	3	10
10	C	1	2	A	B	5	6	7	8	9	3	4	0	C	7	8	9	10	0	1	A	B	4	5	3	6	2
C	3	4	A	B	7	8	9	10	0	1	5	6	2	10	0	1	2	3	4	A	B	7	8	C	6	9	5
5	6	A	B	9	10	0	1	2	3	C	7	8	4	3	4	5	6	7	A	B	10	0	C	2	9	1	8
8	A	B	0	1	2	3	4	5	C	7	9	10	6	7	8	9	10	A	B	2	3	C	5	6	1	4	0
0	9	7	5	3	1	10	8	6	4	2	A	B	C	5	2	10	7	4	1	9	6	3	0	8	A	B	C
3	1	10	8	6	4	2	0	9	7	5	B	C	A	6	3	0	8	5	2	10	7	4	1	9	C	A	B
2	0	9	7	5	3	1	10	8	6	4	C	A	B	1	9	6	3	0	8	5	2	10	7	4	B	C	A

Remark 7.1. For $n \leq 100$ and of the form $4t + 2$ there are three instances where one can utilize either Theorem 6.1 or 7.1 to produce an $O(n,2)$. These orders are 34, 46 and 70 which can be decomposed as follows:

$$34 = 23 + 11 \quad \text{or} \quad 31 + 3$$

$$46 = 31 + 15 \quad \text{or} \quad 41 + 3$$

$$70 = 47 + 23 \quad \text{or} \quad 67 + 3.$$

The natural question to ask now is in what direction should we extend the research on construction of orthogonal Latin squares using the method of sum composition. We would clearly like to investigate the problem of construction of a set $O(n,t)$ for $t > 2$. As a first step in this direction it is necessary to extend the investigations beyond the extreme values of n_2 (see Section 10). The next two smallest values are $n_2 = 4, 5$. As will be seen the composed orthogonal Latin squares for these values of n_2 have a useful statistical application. We delve with these cases in the following two sections.

8. Construction of Two Families of $O(n_1 + 4, 2)$.

It is clear that an exhaustive search for patterns as for $n_2 = 3$ would be very tedious. Our investigations indicate that one could find patterns which would yield a set $O(n_1 + 4, 2)$ for any $n_1 = p^\alpha$ as long as $p \geq 11$ and $\alpha \geq 1$. We shall here present two families of $O(p^\alpha + 4, 2)$ for which either -1 or -2 are quadratic residues in $GF(p^\alpha)$. For both families one has to assume $xy = 1$ in order to obtain distinct solutions for the unknowns in question.

<u>Case 1.</u>	$k_v(s_1, t_1) = t_3$	$k_h(s_1, t_4) = t_2$
	$k_v(s_2, t_2) = s_1$	$k_h(s_2, t_3) = t_4$
	$k_v(s_3, t_3) = t_1$	$k_h(s_3, t_2) = s_4$
	$k_v(s_4, t_4) = s_2$	$k_h(s_4, t_1) = s_3$.

This system of equations will have distinct solutions provided that $3y^2 + 2y + 1 = 0$, i.e., -2 has to be quadratic residue or p has to be of the form $8m + 1$ or $8m + 3$. A system of solutions in terms of t_1 and t_3 are:

$s_1 = yt_1 + (y+1)t_3$	$s_4 = (y+2)t_1 - (y+1)t_3$
$s_2 = -(y-1)t_1 + yt_3$	$t_2 = 2(y+1)t_1 - (2y+1)t_3$
$s_3 = (y+1)t_1 - yt_3$	$t_4 = (2y+1)t_1 - 2yt_3$.

<u>Case 2.</u>	$k_v(s_1, t_1) = t_2$	$k_h(s_1, t_1) = s_2$
	$k_v(s_2, t_2) = s_1$	$k_h(s_2, t_2) = t_1$
	$k_v(s_3, t_3) = t_4$	$k_h(s_3, t_3) = s_4$
	$k_v(s_4, t_4) = s_3$	$k_h(s_4, t_4) = t_3$.

Notice that the four equations of either lines one and two or three and four form a loop. These loops will yield distinct solutions provided that $y^2 + 1 = 0$ or $p = 4m + 1$. A system of solutions is:

$t_2 = (s_1 + yt_1)/(y+1)$	$t_4 = (s_3 + yt_3)/(y+1)$
$s_2 = (t_1 + ys_1)/(y+1)$	$s_4 = (t_3 + ys_3)/(y+1)$.

We may choose the following distinct values for the unknowns:

$$s_1 = 0, t_1 = 1, s_3 = 1 - y \quad \text{and} \quad t_3 = y.$$

Thus we have the following theorem.

Theorem 8.1. Using the method of sum composition it is possible to construct a set $O(p^\alpha + 4, 2)$ for all primes p of the form either $4m + 1$ or $8m + 3$, $p \geq 11$.

Corollary 8.1. The composed $O(p^\alpha + 4, 2)$ has at least 3 common parallel transversals if $p = 11$ and at least 4 common parallel transversals if $p > 11$.

Proof. The original $O(p^\alpha, 2)$ has p^α common parallel transversals. Since $p^\alpha \geq 11$ therefore after removing 8 common parallel transversals we are left with at least 3 common parallel transversals in the corresponding portion of $O(p^\alpha, 2)$ in the composed $O(p^\alpha + 4, 2)$. Now it is known that any $O(4, 2)$ has 4 common parallel transversals. Thus any $t \leq 4$ common parallel transversals of the corner $O(4, 2)$ in the composed set with any t common parallel transversals in the portion corresponding to $O(p^\alpha, 2)$ form three common parallel transversals for the entire set.

Example 8.1. By letting $p = 11$ we can construct an $O(15, 2)$ via sum composition of an $O(11, 2)$ and an $O(4, 2)$. $p = 11$ falls in case 1 and thus $y = 8$, $x = 7$, $S = \{9, 8, 3, 2\}$ and $T = \{0, 5, 1, 6\}$. Utilizing the projection rules given there we obtain the following $O(15, 2)$.

0	1	D	C	4	5	6	7	B	A	10	9	8	3	2
7	D	C	10	0	1	2	B	A	5	6	4	3	9	8
D	C	5	6	7	8	B	A	0	1	2	10	9	4	3
C	0	1	2	3	B	A	6	7	8	D	5	4	10	9
6	7	8	9	B	A	1	2	3	D	C	0	10	5	4
2	3	4	B	A	7	8	9	D	C	1	6	5	0	10
9	10	B	A	2	3	4	D	C	7	8	1	0	6	5
5	B	A	8	9	10	D	C	2	3	4	7	6	1	0
B	A	3	4	5	D	C	8	9	10	0	2	1	7	6
A	9	10	0	D	C	3	4	5	6	B	8	7	2	1
4	5	6	D	C	9	10	0	1	B	A	3	2	8	7
8	2	7	1	6	0	5	10	4	9	3	A	B	C	D
1	6	0	5	10	4	9	3	8	2	7	B	A	D	C
10	4	9	3	8	2	7	1	6	0	5	C	D	A	B
3	8	2	7	1	6	0	5	10	4	9	D	C	B	A

D	C	2	3	4	B	A	7	8	9	10	6	1	5	0
C	9	10	0	B	A	3	4	5	6	D	2	8	1	7
5	6	7	B	A	10	0	1	2	D	C	9	4	8	3
2	3	B	A	6	7	8	9	D	C	1	5	0	4	10
10	B	A	2	3	4	5	D	C	8	9	1	7	0	6
B	A	9	10	0	1	D	C	4	5	6	8	3	7	2
A	5	6	7	8	D	C	0	1	2	B	4	10	3	9
1	2	3	4	D	C	7	8	9	B	A	0	6	10	5
9	10	0	D	C	3	4	5	B	A	8	7	2	6	1
5	7	D	C	10	0	1	B	A	4	5	3	9	2	8
3	D	C	6	7	8	B	A	0	1	2	10	5	9	4
0	4	8	1	5	9	2	6	10	3	7	A	B	C	D
7	0	4	8	1	5	9	2	6	10	3	D	C	B	A
8	1	5	9	2	6	10	3	7	0	4	B	A	D	C
4	8	1	5	9	2	6	10	3	7	0	C	D	A	B

Example 8.2. Considering case 2 and letting $p = 13$ one can construct an $O(17,2)$ by sum composition of an $O(13,2)$ and an $O(4,2)$. In this case $y = 5$, $x = 8$, $S = \{0,11,9,4\}$ and $T = \{1,3,5,10\}$. The detail of construction is left to the reader.

Remark 8.1. Utilizing a different pattern than those considered here, Ruiz and Seiden (1972) have constructed a family of $O(n_1 + 4, 2)$, $n_1 = 1, 2, 3 \pmod{7}$ using $x = 2$ and $y = 5 \pm \sqrt{-7}/4$. One can show that the same result can be obtained by starting with their pattern and assuming that $xy = 1$.

9. Construction of a Family of $O(n_1 + 5, 2)$.

Let us consider the sum composition of $O(p^\alpha, 2)$ based on $GF(p^\alpha)$, $p \geq 11$ and on $O(5, 2)$ based on the following system of projections and capturing the lost transversals.

$$\begin{array}{ll} k_v(s_1, t_1) = t_5 & k_h(s_1, t_1) = s_2 \\ k_v(s_2, t_2) = t_1 & k_h(s_2, t_2) = s_3 \\ k_v(s_3, t_3) = t_2 & k_h(s_3, t_3) = s_4 \\ k_v(s_4, t_4) = t_3 & k_h(s_4, t_4) = s_5 \\ k_v(s_5, t_5) = s_1 & k_h(s_5, t_5) = t_4 \end{array}$$

It can be shown that this system has a solution with distinct components only if $xy = 1$. Otherwise $\sum s_i = \sum t_i$ implies $s_1 = t_4$. Using the condition $xy = 1$ this system will yield a solution with distinct components only if $y^2 + 4 = 0$ in $GF(p)$ which implies -1 has to be a quadratic residue in $GF(p)$, i.e. p has to be of the form $4m + 1$. This system of equations yield the following values for s_i and t_i , $i = 2, 3, 4, 5$ in terms of s_1 and t_1 .

$$\begin{array}{ll} s_2 = [ys_1 + t_1]/(y+1) & t_2 = [(y+2)t_1 - s_1]/(y+1) \\ s_3 = [(y-1)s_1 + 2t_1]/(y+1) & t_3 = [(y+3)t_1 - 2s_1]/(y+1) \\ s_4 = [(y-2)s_1 + 3t_1]/(y+1) & t_4 = [(y+4)t_1 - 3s_1]/(y+1) \\ s_5 = [(y-3)s_1 + 4t_1]/(y+1) & t_5 = [yt_1 + s_1]/(y+1) \end{array}$$

For the choice of $s_1 = 0$ and $t_1 = 1$ the remaining components become

$$\begin{array}{ll}
s_2 = 1/(y+1) & t_2 = (y+2)/(y+1) \\
s_3 = 2/(y+1) & t_3 = (y+3)/(y+1) \\
s_4 = 3/(y+1) & t_4 = (y+4)/(y+1) \\
s_5 = 4/(y+1) & t_5 = y/(y+1) .
\end{array}$$

It is easy to check that the ten values for the unknowns are distinct except for $p = 13$, the smallest prime under consideration. Clearly the values of the sets S and T separately are distinct. As to the differences between the elements of the set S and T

$$s_5 - t_1 = s_4 - t_5 = s_2 - s_4 = 0$$

when $y^2 = 9$ or $13 = 0$. For $p = 13$ we may use the example given in [7] with $x = 2$, $y = 7$, $S = \{0,1,2,3,4\}$ and $T = \{10,11,12,13,9\}$. In this particular case the transversal s_i should be projected on the $(13 + i)$ -th row and column in the order written above. Similarly for the transversal t_i . Thus we have proved the following theorem.

Theorem 9.1. Using the method of sum composition it is possible to construct a set $O(p^\alpha + 5, 2)$ for all p of the form $4m + 1$, $p \geq 13$.

Note that the order of composed Latin squares in Theorem 9.1 is of the form $4t + 2$.

Corollary 9.1. The composed $O(p^\alpha + 5, 2)$ has at least 3 common parallel transversals if $p = 13$ and at least 5 common parallel transversals if $p > 13$.

The proof is analogous to the proof of Corollary 8.1.

Example 9.1. Using the method of Theorem 9.1 we can construct a pair of orthogonal Latin squares of order $18 = 13 + 5$ and a pair of order $22 = 17 + 5$. In the above we exhibited x, y, S and T for 13 and here we present x, y, S and T for case 22.

$$x = 2, y = 9, S = \{0,12,7,2,14\} \quad \text{and} \quad T = \{1,13,8,3,6\} .$$

The exhibition of these squares is left to the reader.

Remark 9.1. For $n = n_1 + n_2 \leq 100$ and of the form $4t + 2$ there are two instances where we can construct an $O(n, 2)$ by either Theorem 7.1 or Theorem 9.1. They are 22 and 94 which can be decomposed in two different ways

$$22 = 19 + 3 \quad \text{or} \quad 17 + 5$$

$$94 = 91 + 3 \quad \text{or} \quad 89 + 5 .$$

10. Discussion Concerning Continuation of Research on the Method of Sum Composition.

We shall discuss a possible extension of the results of this paper in two different directions. The first direction is concerned with the method of sum composition as described here and generalizing the results obtained. The second direction is to modifying the method to obtain the set $O(n_1 + 1, t)$, $t \geq 2$.

As to the first direction we consider the results of this paper a first step in exploring the problem of construction of Latin squares and orthogonal Latin squares via sum composition.

It seems obvious that investigating the problem of construction of orthogonal Latin squares for increased values of n_2 will become overwhelming and uninspiring unless a new method of attack can be found. One possibility may be to choose an especially symmetric pattern which could be generalized to some sets of values of n_2 , say, of specific structure. It seems plausible that for a fixed n_2 one pattern could do for all primes by changing conveniently the value of the function $\frac{1-x}{x-y}$. This amounts to getting away from the assumption $xy = 1$. In fact we did just this in order to complete the case $O(n_1 + 3, 2)$ for all primes.

There is another important reason to consider also cases for which $xy \neq 1$. We aim at construction of sets $O(n, t)$ for $t > 2$. When $t > 2$ there must be at least $O(n, t-1)$ sets for which $xy \neq 1$. Moreover in such a case the sum of the values of the transversals for each of the t sets

must be the same. This reduces considerably the problem of searching for the sets $O(n,t)$.

We may illustrate this idea with the example considered in [7]. We made there an exhaustive search for all pairs of $O(7+3,2)$ with $S = \{0,1,2\}$, $T = \{2,4,5\}$ and not necessarily $xy = 1$. As explained before we must have in such a case $\sum s_i = \sum t_i$. Thus we considered the case $\sum s_i = \sum t_i = 3 \pmod{7}$. It is easy to show that for each of the distinct elements of $GF(7)$ there is just one available pair of $\{S,T\}$ for consideration. Hence in total there are seven pairs to exhaust all possible cases for which $xy = 1$ does not have to hold. For $p = 7$ all the sets are difference sets. The question then arises for which fields will this property hold which could reduce the search even further.

As to the second direction we wish to remark the following: If $B(x)$ and $B(y)$, $x = y^{-1}$ based on Galois field $GF(n)$ form an $O(n,2)$, then it is impossible to construct an $O(n+1,2)$ by sum composition of this $O(n,2)$ and a trivial pair of orthogonal Latin squares of order unity. This is so because it forces S to be equal to T and this can be seen by the fact that S and T each contain one element only, say s and t respectively. Now $k_v(s,t) = (yt+s)(1+y)^{-1}$ will be equal to s or t only if $t = s$, but we require $S \cap T = \emptyset$. However, we believe that with some modifications of the method of sum composition this can be done. Let us look at the following example.

<u>0</u> 1 2 3 4 5 6 7 8	0 1 2 3 4 5 6 7 <u>8</u>
1 <u>3</u> 6 8 7 2 0 5 4	<u>2</u> 5 7 6 1 8 4 3 0
2 6 <u>7</u> 5 1 4 8 3 0	5 <u>6</u> 4 0 3 7 2 8 1
3 8 5 <u>4</u> 0 6 2 1 7	7 4 <u>3</u> 8 5 1 0 6 2
4 7 1 0 <u>2</u> 3 5 8 6	6 0 8 <u>1</u> 2 4 7 5 3
5 2 4 6 3 <u>8</u> 7 0 1	1 3 5 2 <u>7</u> 6 8 0 4
6 0 8 2 5 7 <u>1</u> 4 3	8 7 1 4 6 <u>0</u> 3 2 5
7 5 3 1 8 0 4 <u>6</u> 2	4 2 0 7 8 3 <u>5</u> 1 6
8 4 0 7 6 1 3 2 <u>5</u>	3 8 6 5 0 2 1 <u>4</u> 7 .

These two Latin squares of order 9 are obviously not orthogonal. However, all the cells on the main diagonals or parallel to main diagonals form common parallel transversals. Now let us remove the underlined transversal in each square and project them on the tenth row and column and fill their corresponding cells with 9 and add a 1×1 Latin square in the lower right corner. Thus we obtain.

9	1	2	3	4	5	6	7	8	0	0	1	2	3	4	5	6	7	8	9
1	9	6	8	7	2	0	5	4	3	9	5	7	6	1	8	4	3	0	2
2	6	9	5	1	4	8	3	0	7	5	9	4	0	3	7	2	8	1	6
3	8	5	9	0	6	2	1	7	4	7	4	9	8	5	1	0	6	2	3
4	7	1	0	9	3	5	8	6	2	6	0	8	9	2	4	7	5	3	1
5	2	4	6	3	9	7	0	1	8	1	3	5	2	9	6	8	0	4	7
6	0	8	2	5	7	9	4	3	1	8	7	1	4	6	9	3	2	5	0
7	5	3	1	8	0	4	9	2	6	4	2	0	7	8	3	9	1	6	5
8	4	0	7	6	1	3	2	9	5	3	8	6	5	0	2	1	9	7	4
0	3	7	4	2	8	1	6	5	9	2	6	3	1	7	0	5	4	8	9

The reader can check for himself that these Latin squares of order 10 are orthogonal. Note that these two orthogonal Latin squares have many common transversals all sharing the lower right corner cell. These common transversals can be located on the diagonals parallel to the main diagonal. It is easy to show that this $O(10,2)$ is not isomorphic with our previous $O(10,2)$ derived by composition of an $O(7,2)$ and $O(3,2)$.

The preceeding example indicates a possible modification of sum composition method, viz, starting with non-orthogonal Latin squares. But of course they should have certain combinatorial properties which we could not yet characterize. This matter is under investigation.

Before closing this section we should mention that sum composition with Latin squares of order unity has two important consequences. First, there is

no bound on the number of mutually orthogonal Latin squares of order unity. Secondly, in the process of sum composition we only lose two common parallel transversals for each composition. These are very important if one hopes to construct a set consisting of more than two orthogonal Latin squares by sum composition method.

We wish to thank Mr. W. Allard for searching, with the aid of a high speed computer, for roots of fourth degree equations in some $GF(p)$.

References

1. R.C. Bose, S.S. Shrikhande and E.T. Parker, Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. J. Math.* 12(1960), 189-203.
2. W.T. Federer, Construction of classes of experimental designs using transversals in Latin square and Hedayat's sum composition method, in Statistical Papers in Honor of G.W. Snedecor (edited by T.A. Bancroft), (1972), 91-114, Iowa State University Press.
3. A. Hedayat and E. Seiden, On a method of sum composition of orthogonal Latin squares, RM-238 (1969), Department of Statistics and Probability, Michigan State University.
4. A. Hedayat and E. Seiden, On a method of sum composition of orthogonal Latin squares II, RM-257 (1970), Department of Statistics and Probability, Michigan State University.
5. A. Hedayat and E. Seiden, On a method of sum composition of orthogonal Latin squares III, RM-259 (1970), Department of Statistics and Probability, Michigan State University.
6. A. Hedayat, E.T. Parker and W.T. Federer, The existence and construction of two families of designs for two successive experiments, *Biometrika* 57 (1970), 351-356.
7. A. Hedayat and E. Seiden, On a method of sum composition of orthogonal Latin squares, *Proceedings of the Conference on Combinatorial Geometry and Its Applications*, Perugia, Italy, September 11-17, 1970, 239-256.
8. A. Hedayat, An application of sum composition: A self orthogonal Latin square of order 10, *J. Combinatorial Theory, A* (in press).
9. F. Ruiz and E. Seiden, Some results on the construction of orthogonal Latin squares by the method of sum composition, RM-301 (1972), Department of Statistics and Probability, Michigan State University.